CHAPTER FOUR

INTERNET CONTENT POLICY AND REGULATION IN AUSTRALIA

Peter Coroneos

INTRODUCTION

It can generally be observed that the propensity for creating new internet content regulation within a country results from the interaction of three forces. Firstly, there are the cultural values and institutions within a country. 'Institutions' include the traditional media who have historically acted as drivers of the debate about the harms of being online. Sometimes they are more sensationalist than is justified. In any event, these values and institutions shape the political debate and determine the enthusiasm with which legislatures bring forth new laws, in response, as it were, to public concern.

In Australia, the traditional media have been very active in pointing out the 'dangers' of the internet. To a large degree they have played on the fears of a public which is still coming to terms with the internet revolution. Although the number of Australians online has progressively grown over the last 10 years, from a minority of mainly young, affluent early adopters, to today where the internet is effectively a mainstream medium with almost three quarters of the population online,[1] still the depth of user experience remains thin enough that we see the occasional headline proclaiming the menace of some new internet threat or other.

This is enough to fuel minority groups with their own agendas, to proclaim the internet a risk to traditional values/our children's safety/national security/the future of their business model or whatever

[1] Australian Bureau of Statistics, *Report 8153.0 - Internet Activity* (2007) <http://www.abs.gov.au>.

cause suits them. This may play all the way through to the political level where we eventually see new laws proposed. This dynamic is certainly not unique to Australia, but we have nevertheless seen the mechanism operate here with sometimes startling results.

A variant on this dynamic also applies. Politicians sometimes announce policy positions in response to what they anticipate are popular concerns. The results are the same – new laws, sometimes of questionable utility, but supported for their symbolic and political value. Regrettably, opposition to these policies which are advanced on 'motherhood' grounds is portrayed as a dereliction to duty to children. This tactic has been used to stifle debate and ensure greater cross party support than the problem actually justifies.

A classic example of this process is seen in the lead-up to new legal provisions enacted in 2007.[2] These changes were prompted primarily by a media storm in 2006 centring around the Big Brother so-called 'reality' television show and its related website.

The website streamed content considered more risqué than that which could be broadcast over television. In one now infamous episode, two of the show's participants engaged in behaviour of a nature which many would find offensive, though it fell well short of the kind of typical graphic sexual content available online. The ensuing media sensationalism moved politicians to promise tougher laws to ensure that no future conduct of the nature complained about could be made accessible to minors.

The irony in all this was that there was no evidence that minors had actually accessed the site. By all accounts since it was streamed in the middle of the night, it seems that almost no one saw it live – excerpts were endlessly replayed on television (by competing networks presumably to raise community ire). The lack of demonstrable and widespread public harm did not stop a knee-jerk reaction, made worse by the impending election.

Secondly, the ease with which legislation can actually be enacted in various legal systems will determine the extent to which political activity

[2] *Communications Legislation Amendment (Content Services) Act 2007* (No 124, 2007), <http://www.austlii.edu.au/au/legis/cth/num_act/clasa2007544/> at 14 January 2008.

translates into actual laws. Some legislative systems, such as the US are, by design, resistant to lawmaking. Presidential vetoes, layered committee structures and referral processes serve as a brake on precipitative action, just as the constitutional drafters would have intended.

In other systems, such as Australia's however, the chance outcome of elections and ultimate balance of numbers in the legislature can give a Bill clear passage with only perfunctory scrutiny and debate. That has certainly been our experience in the last three years, and before that deals struck with balance of power interests in the Senate essentially delivered similar outcomes.

Thirdly, constitutional considerations such as guaranteed freedom of expression act as a check on whether, and to what degree, new laws can come into effect, or survive legal challenge. Again, comparing Australia to the US, we have seen examples of laws which have passed in the former only to be struck down on First Amendment grounds.[3]

In Australia's case, no constitutional guarantee for free speech exists, other than that implied by the courts (and confined, in our case, to political discourse). Thus, there is little to be done once a law is passed other than to consider its implementation and its enforcement.

As a result of the interplay of these forces, Australia has been saddled with comparatively strict laws relating to internet content and its access. The following analysis considers why and how these laws have arisen and how they have been implemented in practice.

THE BROADCASTING SERVICES ACT

In Australia, the principal legislation covering internet content is the *Broadcasting Services Act* ('*Act*'). Originally enacted in 1992 to manage issues such as television broadcasting, license conditions and the creation of a statutory regulator the *Australian Broadcasting Authority* (now called the *Australian Communications and Media Authority or ACMA*[4]), the

[3] See for example *Reno, Attorney General of the United States, et al v American Civil Liberties Union et al* 521 U.S. 844 (1996) <http://supreme.justia.com/us/521/844/case.html> at 25 January 2008.

[4] For the remainder of this chapter, the acronym 'ACMA' will be used.

Act has been expanded over time to cover an ever increasing range of content across converging media platforms.

The 1999 amendments to the *Act* extended the powers of the regulator to oversee the transmission and hosting of internet content in Australia.

In large part, the legislation followed the framework outlined by the Federal government in 1997 which articulated the principles ('the Principles')[5] by which online content should be regulated, and was designed as the government's response to a perception that the community, and particularly, Australian children, needed protection from content which was likely to harm them.

The Explanatory Memorandum to the *Act* stated:

> Concern has been expressed both within the community and at government level about the nature of material that may be accessed by means of online services, specifically in relation to the perceived ease of access to material that is either pornographic or otherwise unsuitable for children…
>
> The objective of further proposals is to ensure that the regulatory framework is commensurate with community concerns about online content, particularly that the range of material to be controlled is consistent with the range controlled in conventional media. The Government also considers that the complaints process proposed in 1997 should be revisited to ensure that an unreasonable onus is not placed on service providers and to provide for more timely and efficient handling of complaints to prevent access to material that is of serious concern.

The amendments expanded the Objects of the Act[6] to give voice to three additional purposes:

> (a) to provide a means for addressing complaints about certain Internet content; and

[5] See <http://www.anu.edu.au/mail-archives/link/link9707/0114.html> at 25 January 2008.

[6] Under the Objects clause in s 3 (1) of the *Act*.

(b) to restrict access to certain Internet content that is likely to cause offence to a reasonable adult; and

(c) to protect children from exposure to Internet content that is unsuitable for children.

The attainment of these aims was not absolute, but was qualified according to the following proviso which was also inserted in a new subsection 4 (3) of the *Act*:

> The Parliament also intends that Internet content hosted in Australia, and Internet carriage services supplied to end-users in Australia, be regulated in a manner that, in the opinion of the ACMA:
>
> (a) enables public interest considerations to be addressed in a way that does not impose unnecessary financial and administrative burdens on Internet content hosts and Internet service providers; and
>
> (b) will readily accommodate technological change; and
>
> (c) encourages:
>
> (i) the development of Internet technologies and their application; and
>
> (ii) the provision of services made practicable by those technologies to the Australian community.

These words essentially vested a discretion to the ACMA that allowed it to perform a balancing exercise, something industry later relied upon when seeking to have codes of practice registered.

While it recognised that the internet was difficult to regulate, the government believed that this should not prevent an attempt. There was a view that developing technologies would eventually make this easier, but for now, industry should do all that was feasible.

However, in a significant departure from the 1997 Principles which had recognised that 'on-line service providers … [could not] be held responsible in every case for material they have not created', the

legislation raised the bar to create a default obligation upon ISPs to use *all reasonable efforts to prevent access to content hosted offshore*. This would occur in circumstances where ISPs were notified of the existence of content which the government deemed to be unsuitable for domestic consumption.

For the industry's part, this requirement represented a potential threat to its very existence. ISPs argued that any requirement for them to block offshore hosted content would be expensive and would potentially slow down the Net and the development of the e-commerce in Australia. The availability of circumvention technologies and the inaccuracies of current filter products were also cited as reasons why the legislation would prove ineffective.

Free speech advocates bemoaned the censorship of the only medium that could otherwise guarantee the free flow of expression and political ideas. To them this was a dangerous precedent and triggered swift and vocal international condemnation across the Net. Others found it offensive that one of the Principles articulated by Ministers in 1997 that 'on-line services should not be subject to a more onerous regulatory framework than "off-line" material such as books, videos, films and computer games' should be so wantonly abandoned.

The *default* provisions of the legislation vested in the ACMA the right to issue notices, and to direct ISPs and content hosts to comply with industry standards that would be devised to respond to content of which the ACMA becomes aware. The scheme is complaints driven by design, that is to say, the ACMA would not normally undertake own-motion investigations, but only responds to complaints about Internet content reported to it. It has a discretion to disregard complaints that are in its opinion frivolous, vexatious or 'likely to undermine the administrative processes' of the regime.

The ACMA was also given the power to have content evaluated by an independent body, the Classification Board, and to form views as to whether or not the content ought to be prohibited on that basis.

WHAT TYPES OF CONTENT ARE REGULATED?

Two classes of content are proscribed by the Act: 'Prohibited' and 'Potential Prohibited' content. The first comprises material which is Refused Classification (RC), or is classified X or, in the case of domestically hosted content, is classified R *and* is not also subject to age verification measures.[7] 'Potential prohibited' content is content that has not been classified but were it to be, gives rise to a substantial likelihood that the content would be Prohibited content. This alternative was included to provide the ACMA with the opportunity to undertake quick action, in particular where obviously illegal content (for example child pornography) is reported to it.[8]

Decisions of the ACMA are subject to Administrative Appeal Tribunal merits review, and 'interim' takedown notices in respect of domestically hosted content are reversible where not subsequently found by the Classification Board to be prohibited.

The *Act* defines 'internet content' to include information that:

(a) is kept on a data storage device; and

(b) is accessed, or available for access, using an Internet carriage service;

---

[7] Further amendments to the *Act* in 1997 have extended Prohibited Content to include MA15+ content where it is provided in the form of video as part of a commercial content service (other than news or current affairs) and not subject to a restricted access system to prevent persons under the age of 15 years from accessing it.

[8] The following categories of Internet content are prohibited for hosting on servers within Australia:

> Content which is (or would be) classified RC or X by the Classification Board. Such content includes: material containing detailed instruction in crime, violence or drug use; child pornography; bestiality; excessively violent or sexually violent material, real depictions of actual sexual activity; and
>
> Content hosted in Australia which is classified R *and is not subject to a restricted access (eg. age verification) system* which complies with criteria determined by the ACMA. Content classified R is not considered suitable for minors and includes: material containing excessive and/or strong violence or sexual violence; material containing implied or simulated sexual activity; or material which deals with issues or contains depictions which require an adult perspective.

> but does not include information that is transmitted in the form of a broadcasting service.

This appears to be a very broad definition; however it was circumscribed by the exclusion of email, live (ephemeral) content, newsgroups and FTP traffic.

The justification for these carve outs related to either the private nature of communications, in the case of email and FTP traffic, or the temporary nature of the content in the case of live streams, chat, and posts to newsgroups. Since neither private nor temporary content is really that conducive to the complaints-based approach taken in the *Act*, the government conceded that inclusion of these elements would add little to the scheme beyond making it harder to enforce.

IMPLEMENTING THE BROADCASTING SERVICES ACT

The preceding analysis might suggest that the legislation would be in practice as draconian as some have feared. But in the period since its implementation, events have proved otherwise. The key elements which ameliorate the least workable aspects of the legislation are to be found in the concessions to industry secured by last minute amendments negotiated primarily by the IIA on behalf of the industry, and supported by both the Government and the Opposition in the Senate.

Most important of all are the provisions in the *Act* which allowed for the development of an alternative scheme which substitutes for externally imposed regulatory action, particularly in regard to blocking of content hosted offshore. The legislation allowed for industry to develop so-called 'alternative access prevention arrangements' though registered codes of practice. As a result, the ACMA's role was has been largely limited to domestic content, with industry's own approach determining the practical day-to-day obligations of ISPs. The modified regime does not require any form of self-censorship or pre-emptive action on the part of ISPs.

R-rated content is allowed to be hosted in Australia, provided it is behind some form of age verification mechanism. The ACMA settled on

a combination of credit card details and the use of a PIN to constitute a *de facto* age barrier. The latter is issuable upon provision of sufficient personal information by the user to allow the issuer (that is, the adult content provider), a reasonable degree of confidence about age.

While this is consistent with the practice of adult sites operating overseas, in our view the exercise has become somewhat academic since the small amount of adult content which was previously hosted in Australia has largely moved to the constitutionally protected hosting sites in the US, or other jurisdictions.[9]

CO-REGULATION AND THE INTERNET INDUSTRY ASSOCIATION CODES OF PRACTICE

How they do these industry codes, which now form such a central part of Australia's online content regulatory regime, actually work?

To answer this question, it is first necessary to understand the concept of co-regulation as it applies in Australia. Under our co-regulatory model, which arose from the 1991 deregulation of the telecommunications sector, industry first develops codified rules to address known consumer risks. In some cases consumer representatives form part of the code-making process, sometimes not. In any event, a public consultation process follows the publication of draft codes, after which time the relevant government regulator evaluates them to ensure they provide adequate community safeguards and have addressed issues raised during the consultation. Once the regulator approves the codes, they become enforceable as if they were law. There are substantial penalties for non-compliance, brought by the regulator and enforceable usually in the Federal Court of Australia.

The IIA took advantage of the degree of self determination afforded by the legislation under the doctrine of co-regulation to develop three

[9] According to figures provided by the ACMA to the Australian Senate Estimates Hearings in November 2000 for example, after almost a year after the operation of the scheme, only 99 items of content had been ordered off Australian-based servers where they had been hosted.

content Codes of Practice.[10] These were registered with the ACMA in December 1999, after the requisite consultation with the public and with NetAlert, the community advisory body established under the *Act*.

In broad terms, we sought to achieve the primary objective of protecting children by requiring industry to make available to end-users the means of controlling content.[11] The Codes operate as the *de facto* standards by which industry meets its obligations under the online content laws. They are co-regulatory in nature because they are developed by industry and enforced by government.

We described the approach taken within the Code as 'industry facilitated user empowerment'. The solution is designed to achieve the broad objectives of the legislation without any significant burden on or damage to the industry. The key elements of our approach include:

- legal assessments and determinations to be made by authorities experienced and resourced to do so
- education of and responsibility by parents, supported by industry
- encouraging the use of technological tools such as content filters and labelling.

It is important to note that the Codes do not impose any requirement for ISPs to engage in universal blocking of content which the ACMA deems prohibited. Rather, they require that ISPs provide end users with tools by which means they can control the access to content in the home. Schedule 1 of the Code, which was compiled after the completion of an independent evaluation of available options, identifies a range of access prevention technologies from which ISPs can select to satisfy the requirements of the Code. ISPs are not expected to absorb the costs associated with meeting this obligation. Market forces determine how

[10] Available at <www.iia.net.au>. There are three industry codes because the *Act* stipulated that up to three codes could be developed, one for ISPs providing access to offshore content, one for ISPs providing access to locally hosted content, and one for internet content hosts. These distinctions are somewhat academic given the crossover areas of activity involved. Code and Codes are used interchangeably here because the three Codes are really three codes in one.

much, if any, of the costs are passed on to end users. However, a later iteration of the Codes in 2002 introduced a further requirement that filters be supplied to users on a cost recovery basis, to keep costs to a minimum.

The suppliers of the alternative access prevention technologies (for example, filter products) who in most cases are *not* the ISPs themselves, are required to update their products and services to filter any additional material which the ACMA has classified as prohibited. The providers of the technologies are also expected to support those technologies though the provision of help lines, online FAQ's and the like. It was not the intention of the IIA in developing the Codes, that ISPs be burdened with that task, unless ISPs themselves choose to develop and have accredited access control measures for use with their own (applicable) customer base.

The registration of the IIA Codes ensures that ISPs in Australia are not required to respond to 'access prevention notices' as provided for by the default provisions of the *Act*. Indeed, such notices have not seen the light of day, precisely because the alternative (Code) scheme is in place.

In cases where material of an obviously serious nature (such as child pornography) is referred to the ACMA, the Authority will independently inform relevant law enforcement agencies in the host country through the appropriate channels. Apart from that, the industry developed Code alternatives have entirely bypassed the need for ACMA to act in respect of internationally hosted content.

For content hosts, the Code requirement of most significance is that they remove, upon notification by the ACMA, prohibited or potential prohibited content which they host in Australia. This reflects the default obligation in the legislation.[12] As is the case for ISPs, content hosts do not have to act pre-emptively, for example in vetting content for suitability, and under the legislation are protected from civil liability when acting in accordance with a takedown notice.[13] This protection accords with the IIA's long-argued view of the need for safe-harbour for

[12] See generally Clause 37 of Schedule 5 of the amending legislation.

[13] This is provided for under subclause 88(3) of the Schedule; ISPs are protected under subclause 88(1) where they deal with content in accordance with a registered code's procedures in relation to content.

responsible industry behaviour, and reflects similar approaches in the US.[14]

Other empowerment strategies, prescribed by the legislation and embodied in the Codes, involve the provision of information to end users by ISPs and hosts. The Codes stipulate the information that must be provided and contain deeming provisions, whereby ISPs and hosts can comply simply by hyperlinking their sites to an online resource created for the purpose by the IIA.[15]

In 2002, to further promote the empowerment solutions central to the Codes, the IIA introduced the Family Friendly ISP scheme. This licensed-based scheme entitles Code-compliant ISPs to display a 'ladybird' seal on their sites, signifying to families their entitlement to the kind of protection and assistance that the Codes mandate. Clicking on the seal takes the user to a page where they can find out about options for online safety and, if desired, obtain a filter. In the three years since the scheme commenced, over 75% of Australian internet users are now serviced by ISPs bearing the Ladybird, and that number continues to grow. The scheme is supported and promoted by NetAlert which continues in its role as a community advisory body funded by government, and since 2007 has become part of ACMA. This collaboration ensures a consistency of message to end users about options available to them.

THE 2005 AMENDMENTS TO THE IIA CODES: ADDRESSING MOBILITY AND CONVERGERNCE

In late May 2005, the ACMA approved further iterations to the IIA Codes which for the first time saw an industry-wide response to the emerging issue of mobile internet content.

The changes were in response to the IIA's monitoring of the convergence of mobile and internet technologies for the previous 18 months, along with local and international market trends and increasing

[14] For example, ISP acts done in accordance with the *Digital Millennium Copyright Act* 1998.
[15] The relevant resource can be found at <www.iia.net.au/guideuser.html>.

interest by regulators in the emerging risks. Accordingly, the IIA determined it was timely to develop a proactive, workable industry response to the question of children's access to multimedia and internet content via mobile devices.

The new provisions within the Codes require mobile content providers to assess content that is to be hosted within Australia to ensure that it complies with appropriate classification standards. Content which would likely be rated MA (for mature audiences) or stronger must be subject to restricted access systems which require age verification and opting in by customers wishing to access this content.[16]

In addition, the Family Friendly Scheme was extended to cover internet content hosts and mobile carriers who are Code-compliant. Filter companies whose solutions pass an independent testing process are also entitled to display the Ladybird seal, and to designate their products as 'Family Friendly Filters', thus tying all elements of the scheme together into a coherent and recognisable symbol of family protection.

RECENT CHANGES TO THE LAW

Further amendments in 2007 to the *Act* however, have expanded the range of subject matter to be regulated to include content accessible via mobile devices, and removed the exemption for live content by seeking to regulate live content *services*.

[16] It should be noted that pursuant to a Ministerial direction in 2004, the Australian Communications Authority on 29 June 2005 issued the Telecommunications Service Provider (Mobile Premium Services) Determination 2005 (No 1). This instrument applies to both carriage service providers and content providers due to the respective roles in delivering mobile content to users. There is some crossover with the *Broadcasting Services Act* and IIA Codes, but being both aware and involved in the industry response during the development of the determination the IIA ensured that the Codes registered by the ACMA were not inconsistent with the requirements of the determination – so as not to expose industry to an incompatible set of requirements. In view of the subsequent merger of the ACMA and the ACA and the passage of the *Content Services Act* amendments in 2007, it is our expectation that there will be a rationalisation of the two regimes within the next few months to simplify the regulatory landscape under which the mobile content industry now operates in Australia.

Age verification was extended to content rated MA15+ - that is, content suitable for persons aged 15 years and older. This applies to commercial content services and video services with an 'Australian connection' (that is, hosted or originating in Australia).

Again, exemptions for certain classes of content were introduced to limit the application of the *Act*. These included (as with the 1999 amendments) broadcasting services, as well as news and current affairs services; search engines, user-based content services, online trading services, voice and video calls with other end-users, SMS services, data storage and back-up services, and services specified in the regulations (giving the Minister the power to declare additional exempt classes of content or services).

A commercial nexus test which was introduced to bring certain activities into the ambit of the *Act* was reformulated during the drafting process (following pressure from industry) to exclude advertising based business models and billing relationships – so that effectively only subscription based or fee-for-content services are caught.

Mobile devices are not amenable to filtering at the device level. Most proprietary content for premium mobile services is hosted in Australia (generally developed by third party providers and supplied under contract to mobile carriers). This proprietary content is hosted within a 'walled garden' and available only to users of a particular mobile phone service.

This distinguishes the content from that which is generally available over the internet, and accessible via mobiles. For this, there is no current regulation other than takedown if that content is deemed to be prohibited content by the regulator *and* hosted in Australia.

Because of the degree of control that mobile carriers have over the content held within their own walled gardens, it was realised that the lack of filtering could be overcome by a generalised obligation to pre-classify content and take down content which might be subsequently complained about.

This is the case in relation to MA15+ content. The measures were codified in the Mobile Premium Services Initiative (which responded to

the Mobile Premium Services Determination which had been pronounced by the Australian Communications Authority).

There remain some residual challenges with the new laws which were not addressed in the amendments. In particular, user generated content potentially presents a liability for content hosts where they do not determine the content, and where no age verification is in place. This is made more complex by the requirement for age verification for MA15+ content. In the absence of a uniform age identifier, it is difficult to see how this can be achieved. Industry is proposing a number of surrogate measures to give effect to the policy intent while still allowing services to operate without disadvantage when compared to overseas counterparts. It remains to be seen if these are accepted by ACMA.

NEW DEVELOPMENTS

In spite of the continuous efforts by industry to ward off obligations for mandatory server level filtering, recent political developments suggest that some form of server based filtering will become mandated in Australia in the near future. Australia is currently preparing for a general election to be held in late November 2007.

Depending which political party wins the election, ISPs will be required to either:

- Offer the option of a filtered service to users; or
- Filter all content prior to access by users, with 'adult' content available on an opt-in basis.

These policies are not clearly defined, suggesting that the Parties may be prepared to compromise on the basis of technical and practical concerns which are likely to emerge once the election is over and the time comes for implementation.

For its part, the present Government has announced a suite of policies of which ISP filtering is only a small part. The major initiative is in fact the free distribution of client side (that is, PC based) filters for installation by end users at home which has been funded to the tune of some AU$89 million, making it the largest empowerment measure of its kind in the world. The intent is to provide families with appropriate

technology to assist in limiting the inadvertent access by children to unsuitable material. [17] Industry generally supports these measures, particularly since the cost is entirely borne by the government and there is no impact on the network.

The Opposition party has a policy which is more far-reaching. Based on the Cleanfeed project announced in the UK in 2004, the intention is for all content to be filtered by ISPs according to a list prepared by the government regulator.

There is hostility to this policy from industry and free speech advocates, the former concerned about effect on network performance and unintended consequences, and the latter concerned about the lack of transparency inherent in the process of list formation and disclosure. While the intent seems to be for child abuse images to be filtered, consistent with regulation and industry practice in Europe and Scandinavia, there are some indications that the content categories could be broader. Specifically, the Shadow Minister has suggested in policy statements that *all* adult content should be blocked by default, and only made accessible on request to the ISP by an adult account holder.

CONCLUSION

The history of internet content regulation in Australia is testimony to the highly politicised nature of the issues. On the one hand we have seen more and more restrictions being legislated. Concurrent with this has been the unprecedented rise in the dependence on the internet by ever increasing numbers of Australians. While successive ministries have sought to respond to community concern by being 'tough on internet pornography' and have campaigned using slogans like 'cleaning up the Net' the reality for most Australians is that they can access the same range of content that they always could. What has really changed are the profile and availability of empowerment tools for families. This suggests that the politicians are more interested in the symbolic power of regulation and it has been left to industry working with the regulator to translate tough laws into workable solutions. In spite of this, more

[17] More information about this scheme is available at <www.netalert.gov.au>.

recent developments suggest a more interventionist approach to ISP responsibility, following events such as Cleanfeed in the UK, and ISPs in other European jurisdictions now voluntarily filtering child abuse images.

It will become clearer in coming months whether Australia is truly moving to greater reliance on intermediaries (that is the connectivity providers) to protect internet users from the perceived harms of the internet, or whether the focus will remain on end user empowerment and education. Ultimately, it is hard to avoid the conclusion that we will be left with a mix of these elements, signalling that the traditional role of common carriers and mere conduits may be drawing to an end.[18]

[18] For further online references see *Broadcasting Services Act 1992* (Cth) <http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/> at 25 January 2008; Australian Communications and Media Authority (formerly ABA) <http://www.acma.gov.au>; Classification Board <http://www.classifcation.gov.au/special.html> at 25 January 2008; IIA Content Codes of Practice <http://www.iia.net.au/index.php?option=com_content&task=category&sectionid=3&id=19&Itemid=33> at 25 January 2008; IIA Guide for ISPs <http://www.iia.net.au/guide.html> at 25 January 2008; IIA Guide for Families (including information about the Family Friendly Scheme) <http://www.iia.net.au/guideuser.html> at 25 January 2008; NetAlert <http://www.netalert.gov.au>; Telecommunications Service Provider (Mobile Premium Services) Determination 2005 (No 1) <http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrument1.nsf/all/search/CD4F1D276DF634C0CA25702F0009DAC0> at 25 January 2008.